



EDP Group's Risk Governance Model

EDP Group's Risk Governance Model

- The **General and Supervisory Board (GSB)**, in particular the Financial Matters Committee/ Audit Committee, is responsible for permanently monitoring the effectiveness of the risk management system, namely in terms of identifying, evaluating, controlling and managing risks and assessing the degree of internal compliance with the company's risk management system. The GSB continuously monitors its performance and effectiveness, in conjunction with the Executive Board of Directors, namely risk control policies, the identification of key risk indicators (KRI) and integrated risk assessment methodologies, and must assess and comment on the EDP Group's strategic lines and corporate risk management policy prior to their final approval by the Executive Board of Directors.
- The **Executive Board of Directors (EBD)** is ultimately responsible for deciding, supervising, and controlling risk management, and is responsible for setting the EDP Group's management objectives and policies. Its main responsibilities are (i) to provide the Business Units and Platforms with adequate resources for an efficient risk management activity, (ii) to formally appoint those responsible for the day-to-day management of relevant risks (risk-owners) and those responsible for energising risk management (risk-officers); (iii) approving and supporting the implementation of Risk Committees for the Business Units and Platforms, whenever the materiality or nature of the risks covered so justifies, (iv) ensuring that the risks within the scope of its activity are identified, analysed and assessed in a comprehensive, rigorous and consistent manner at Group level, in line with the methodologies established by the Risk Units, (v) monitoring the evolution of the main risks of its activity and control limits, periodically assessing the effectiveness of existing risk controls, (vi) providing adequate visibility of relevant aspects of risk management, (vii) defining the Risk Appetite set out in the Business Plan, (viii) defining risk policies for the EDP Group (namely the respective exposure limits by risk category) and (ix) allocating resources according to the risk-return profile of the various options available.
- The **Risk Global Unit (RISK)**, headed by the Chief Risk Officer, performs a function independent of the conduct of the business and supports the Executive Board of Directors at the level of the second line of defence. Its mission is to promote an integrated view of the EDP Group's risk, ensuring the alignment of risk policies and limits with the appetite defined for the Group and coordinating risk-return studies at Group level, with the aim of supporting the Executive Board of Directors in monitoring and mitigating the main risks. Its main responsibilities are (i) defining concepts, methods, risk measures and key risk indicators (KRI), in accordance with best practices and promoting an integrated and harmonised vision of risk in the Group, (ii) updating the Corporate Risk Management Policy and Manual, (iii) maintaining and updating the taxonomy of the Group's most significant risks and promoting their implementation in the various Business Units and Corporate Divisions, (iv) promoting and monitoring the Risk Appetite framework, ensuring consistency with the strategy, and monitoring and reporting conclusions and any non-compliance to the Executive Board of Directors, (v) identifying and reporting the need to define new policies, limits or adjustments to the exposure limits already established by the Executive Board of Directors, as well as solutions for better risk-return management, (vi) the development of significant risk assessment projects and risk-return analyses together with the risk officers of the Business Units and Platforms, (vii) the quantification and

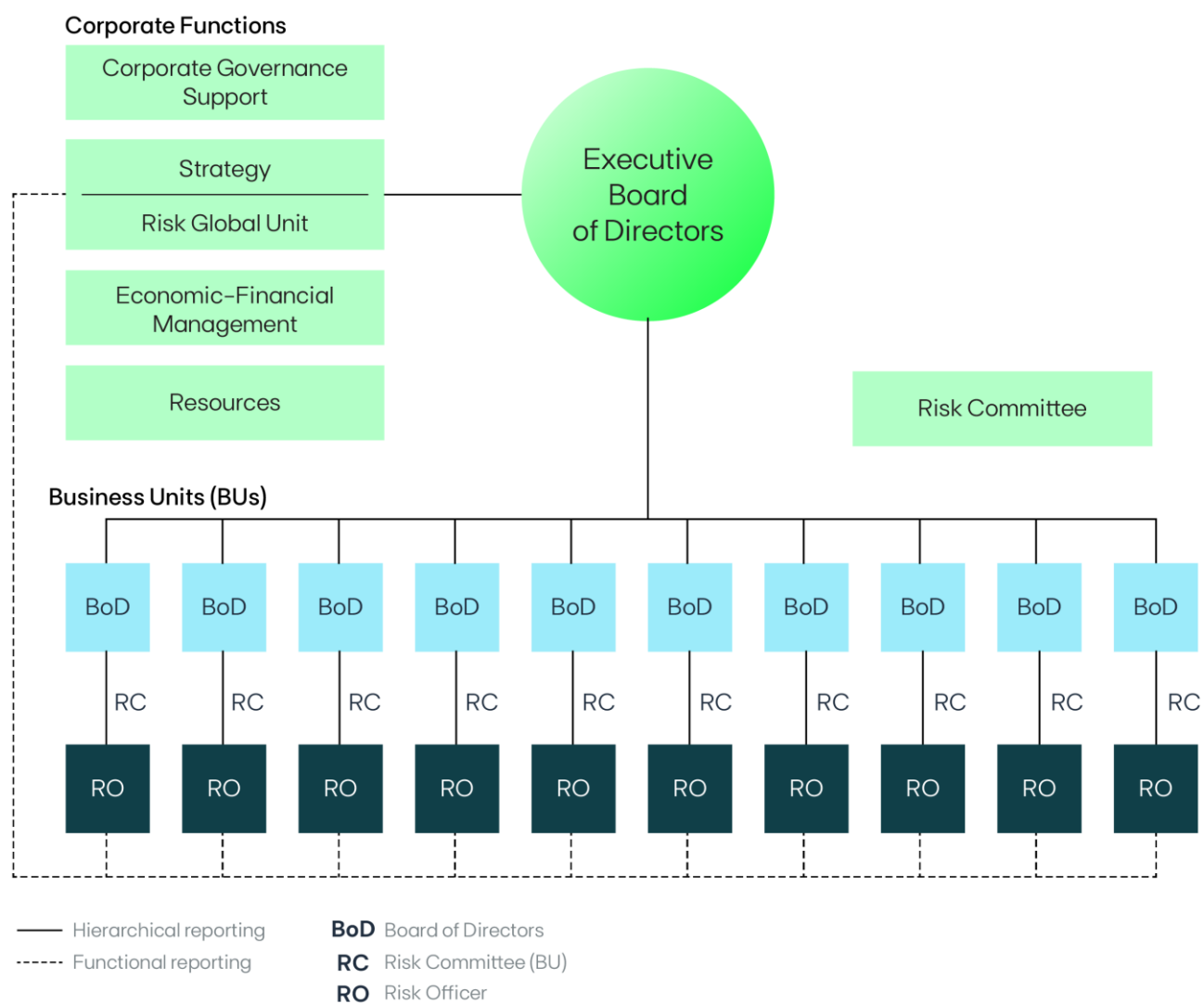
qualification of the materiality of the risks of the Business Units or platforms, together with the different ROs of the BUs, (viii) the dialogue and adequate flow of information to and from the local risk officers, decision-making bodies and other relevant stakeholders in all pertinent matters relating to risk, (ix) promoting the process of monitoring the main risks (recurring and structural monitoring) and reporting to the Executive Board of Directors on the evolution of their level of exposure and contrast with established limits and (x) promoting a culture of risk management across the Group.

- The **risk-owners** of the Business Units and Corporate Divisions are all the business managers who assume risk in their day-to-day activities and act in accordance with the defined risk strategies. From a risk perspective, they must coordinate their activity with the risk-officer of the Business Unit/Platform, and are responsible for (i) implementing mitigation measures and treatment plans in accordance with what is defined in the risk policies, (ii) monitoring the risk indicators defined (KRIs) by RISK, (ii) monitoring the risk indicators defined (KRIs) by RISK, reporting on their evolution and giving visibility to the Business Unit/Platform risk-officer whenever there is or is anticipated any behaviour that could compromise the defined risk strategy and (iii) collecting and reporting risk information to the risk-officer, within the scope of their activity, in accordance with recurring activities (risk maps, reports, among others) or whenever necessary.
- The **local structures for risk management (risk-officers)** play the main role in operationalising risk management and are typically under the direct hierarchical dependence of the respective Board of Directors, with functional coordination with the Group's Chief Risk-Officer, acting in a segregated manner and independent from the conduct of the business. In the Business Units where the respective size and/or complexity justifies it, the corporate risk management structure is replicated at local level, in close articulation with it. Its responsibilities include (i) following the risk management methodology defined for the Group, (ii) identifying the main risks (threats and opportunities), within the scope of the activity and in close coordination with those responsible for the business, (iii) characterising the main risks, quantifying and qualifying their materiality, (iv) escalate material risks to its Board of Directors and to RISK, (v) carry out studies on the main strategic issues and associated risks, in close liaison with those responsible for the business and RISK, (vi) support its Board of Directors in making strategic decisions from a risk perspective, (vii) propose or give an opinion on ways of mitigating or covering the main risks, including, where applicable, the definition of risk management policies, risk treatment guidelines and risk limits, in conjunction with RISK, (viii) following up and monitoring relevant risks by drawing up periodic risk exposure reports and disclosing them to decision-making bodies and Risk, as well as monitoring the implementation of policies, risk management policies, standards and procedures, including monitoring exposures in relation to established limits, (ix) coordinating meetings of the Risk Committees, (x) ensuring dialogue and the appropriate flow of information to and from Risk, decision-making bodies and other relevant stakeholders on all relevant risk-related matters.

The Governance Model of EDP Group, as well as overall the Enterprise Risk Management (ERM) framework, is supported by EDP's Group Risk Management Policy, which is aligned with international best practices (ISO Standard 31000, and COSO-ERM framework). The ERM framework of EDP Group is in continuous improvement, and the last external audit took place in 2022 and focused on assessing the level of maturity of the Enterprise Risk Management system at group and Business Unit levels (assessing ERM framework maturity and identify opportunities for improvement in relation to the reference standards and practices, namely the identified previously).

Within the organization, there is a performance evaluation model for employees that influences short-term incentives. This performance model is designed to assess and enhance employee contributions towards the organization's goals. The model encompasses performance indicators related to various risk areas, including safety, digital, financial and compliance. By doing so, it ensures a comprehensive approach that aligns with the organization's strategic objectives and standards of excellence. Employees contribute to this model by striving to meet and exceed these performance indicators in their tasks, thereby directly influencing their performance evaluations and the corresponding short-term incentives. This approach not only motivates employees to perform at their best but also promotes a culture of accountability and continuous improvement within the organization.

EDP Group's Risk Governance Model (and dialogue with the corporate center)



In addition, there are a number of regular forums for debating, analysing and issuing opinions on risk issues:

- The EDP Group's **Risk Committee** main objective is to support the decisions of the Executive Board of Directors in the identification, analysis, assessment, treatment and monitoring of risk, and it is responsible for (i) supporting the identification of

significant risks and the characterisation of the EDP Group's risk-return profile, (ii) discuss the results of projects analysing and assessing significant risks developed jointly with the Business Units and Corporate Divisions, (iii) propose and issue opinions and/or recommendations on strategies for managing significant risks (e.g. in terms of policies, procedures and limits) for consideration and approval by the Executive Board of Directors and (iv) monitor and control the evolution of significant risks. This Committee meets periodically and, whenever necessary, extraordinarily, preferably at least quarterly. The Committee is made up of the main decision-makers and those responsible for the Group's risk management (members of the Executive Board of Directors, key corporate areas and members with responsibility for risk management of the main platforms/geographies).

- **Local Risk Committees** are set up and run at the level of the Group's Business Units when the degree of complexity of risk management justifies it. They have a structure replicated from the Group's RISK Committee. These Committees are typically coordinated by the respective risk-officer and are attended by members of the Board of Directors, key areas of the Business Unit, as well as a member of RISK, to ensure alignment at Group level.